The following is claimed:

Sub A2

1. A system for providing electronic security for an internal resource capable of capable of communicating via an external communications network, the system comprising:

a server having a first set of ports for communication between the external communications network and the server; the server having a second set of ports for communication between an internal communications network and the server;

a first firewall in communication with the first set of ports and interposed to provide at least one interconnection between the first set of ports and the external communications network; and

a second firewall in communication with the second set of ports and interposed to provide a nonnegative integer number of interconnections between the first set of ports and the internal communications network.

2. The system according to claim 1 wherein the first firewall has outer ports and the second firewall has inner ports, the outer ports of the first firewall having different port identifiers than the inner ports of the second firewall such that a progression of an unauthorized incoming data message that traverses an interconnection via one of the outer ports of the first firewall is blocked at the inner ports of the second firewall.

3. The system according to claim 1 wherein the first firewall has ports and interconnections dedicated to supporting corresponding functions, such that the first firewall blocks a transmission of an incoming data message through the first firewall if a received port identifier of the data message does not coincide with a reference port identifier of an input port supporting a desired functionality of the server for processing the data message.

4. The system according to claim 1 wherein the first firewall includes a primary interconnection for supporting Hypertext Transfer Protocol traffic, a

second interconnection dedicated to encrypted Hypertext Transfer Protocol traffic, a tertiary interconnection dedicated to monitoring a server, and a quaternary interconnection for monitoring operations and maintenance of the internal resource affiliated with the internal communications network.

SWA37

5. The system according to claim 1 wherein the second firewall has interconnection is only established for a limited duration on an as-needed basis for communications between an internal resource of one business entity and another business entity.

6. The system according to claim 1 wherein first firewall and the second firewall comprise software instructions for execution by the server.

7. The system according to claim 1 wherein the at least one interconnection of the first firewall is associated with a first port identifier, the nonnegative integer number of interconnections of the second firewall being associated with one or more second port identifiers, the at least one first port identifier being different from the second port identifiers for each active interconnection.

8. The system according to claim 1 wherein the second firewall blocks a communications message, where a user of the external communications network attempts to use a first port identifier associated with an interconnection of the first firewall to penetrate the second firewall having a second port identifier distinct from the first port identifier.

9. The system according to claim 1 wherein the interconnection represents a communicative state in which communications flow through one of said firewalls and wherein a lack of an interconnection represents a blocked state in which communications are blocked from traversing through one of said firewalls.

10. The system according to claim 1 wherein the nonnegative integer number of interconnections represents zero for a high security mode.

11. The system according to claim 1 wherein the nonnegative integer number of interconnections represents a greater number or equal number to the at least one interconnection during a normal security mode.

12. The system according to claim 1 wherein the external communications network comprises the Internet.

13. A system for providing electronic security for an internal resource capable of communicating via an external communications network, the system comprising:

a server having a first set of ports for communication between an external communications network and the server; the server having a second set of ports for communication between an internal communications network and the server;

a first firewall in communication with the first set of ports and interposed to provide at least one interconnection between the first set of ports and the external communications network, the first firewall having inner ports; and

a second firewall in communication with the second set of ports and interposed to provide a nonnegative integer number of interconnections between the first set of ports and the internal communications network, the second firewall having different port identifiers than those of the first firewall.

14. The system according to claim 13 wherein a number of interconnections of the first firewall is less than or equal to the nonnegative integer number of interconnections of the second firewall.

15. The system according to claim 13 wherein the first firewall blocks a transmission of an incoming data message through the first firewall if a received port identifier of the data message does not coincide with a reference port identifier, the first firewall that supports a desired functionality of the server for processing the data message.

16. The system according to claim 13 wherein the first firewall has inner ports associated with a primary interconnection, a secondary interconnection, a tertiary interconnection, and a quaternary interconnection, the primary interconnection supporting Hypertext Transfer Protocol traffic, the secondary interconnection dedicated to encrypted Hypertext Transfer Protocol traffic, the tertiary interconnection dedicated to monitoring a server, and the quaternary interconnection arranged for monitoring operations and maintenance of the internal resource affiliated with the internal communications network .

17. The system according to claim 13 wherein the second firewall has interconnections that are only established for a limited duration on an as-needed basis for communications between an internal resource of one business entity and another business entity.

18. The system according to claim 13 wherein first firewall and the second firewall comprise software instructions for execution by the server.

19. The system according to claim 13 wherein the at least one interconnection of the first firewall is associated with a first port identifier, the nonnegative integer number of interconnections of the second firewall being associated with one or more second port identifiers, the at least one first port identifier being different from the second port identifiers for each active interconnection.

20. The system according to claim 13 wherein the second firewall blocks a data message from traversing the second firewall, where the user attempts to use a first port identifier associated with an interconnection of the first firewall to penetrate the second firewall having a second port identifier distinct from the first port identifier.

21. A method for providing security for an electronic transaction between entities over a communications network, the method comprising the steps of:

preparing a data message associated with a source address of a second data processing system and a destination address of a first data processing system;

annotating the data message with a first port identifier associated with a first firewall and a second port identifier associated with a second firewall, wherein the first port identifier is distinct from the second port identifier;

determining if the sent first port identifier matches a reference first port identifier of the first firewall; and

handling a data message by the first firewall based on an outcome of the determining step.

22. The method according to claim 21 wherein the handling step comprises passing the data message through the first firewall if the determination finds that the sent first port identifier matches the reference first port identifier.

23. The method according to claim 21 wherein the handling step comprises blocking the passage of the data message through the first firewall if the determination finds that the sent first port identifier does not match the reference first port identifier.

24. The method according to claim 21 further comprising the step of:

deciding if the sent second port identifier matches a reference second port identifier of the second firewall; and

processing the data message by the second firewall based on an outcome of the deciding step.

25. The method according to claim 24 wherein the processing step comprises passing the data message through the second firewall if the outcome is that the sent second port identifier matches the reference second port identifier.

26. The method according to claim 24 wherein the handling step comprises blocking the passage of the data message through the second firewall if the

outcome is that the sent second port identifier does not match the reference second port identifier.

27. The method according to claim 21 further comprising the step of:

deciding if the sent source address matches a reference source address of the second firewall; and

processing the data message by the second firewall based on an outcome of the deciding step.

28. The method according to claim 27 wherein the processing step comprises passing the data message through the second firewall if the outcome is that the sent source address matches the reference source address.

29. The method according to claim 27 wherein the handling step comprises blocking the passage of the data message through the second firewall if the outcome is that the sent source address does not match the reference source address.